CLAIMS

What Is claimed Is:

1. A method to encipher a plaintext, comprising:

enciphering the plaintext with a weak, wide-blocksize block cipher to produce an intermediate value;

masking the intermediate value to produce a masked intermediate value; and

deciphering the masked intermediate value using a weak, wide-blocksize, block cipher.

2. A method as recited in claim 1, wherein the weak, wide-blocksize block cipher is a mode of operation of a conventional block cipher.

3. A method as recited in claim 1, wherein at least one of said steps depends on a tweak.

4. A method as recited in claim 1, wherein said masking step uses multiplication in a finite field.

5. A method as recited in claim 1, wherein said masking step uses a mask obtained by XORing together portions of the intermediate value.

6. A method to encipher a plaintext into a ciphertext, comprising:

forming an intermediate value by enciphering the plaintext with a first, weak block cipher that is keyed using a key;

masking the intermediate value to produce a masked intermediate value; and

computing the ciphertext by deciphering the masked intermediate value using a second, weak, block cipher that is keyed using said key.

7. A method as recited in claim 6, wherein the weak, block cipher is a mode of operation of a conventional block cipher.

8. A method as recited in claim 6, wherein at least one of said steps depends on a tweak.

9. A method as recited in claim 6, wherein said masking step uses multiplication in a finite field.

10. A method as recited in claim 6, wherein said masking step uses a mask obtained by XORing together portions of the intermediate value.

11. A method to encipher a plaintext into a ciphertext, comprising:

enciphering the plaintext with a weak block cipher to form an intermediate value;

masking the intermediate value; and

enciphering the intermediate value with a weak block cipher.

12. A method as recited in claim 11, wherein the weak block cipher is a mode of operation of a conventional block cipher.

13. A method as recited in claim 11, wherein at least one of said steps depends on a tweak.

14. A method as recited in claim 11, wherein said masking step uses multiplication in a finite field.

15. A method as recited in claim 11, wherein said masking step uses a mask obtained by XORing together portions of the intermediate value.

16. A strong, wide-blocksize block cipher for enciphering a plaintext into a ciphertext, comprising:

computing an intermediate value by enciphering the plaintext with a first, weak, wide-blocksize block cipher;

forming a mask from at least the intermediate value;

combining the intermediate value and the mask to produce a masked intermediate value; and

computing the ciphertext by deciphering the masked intermediate value using a second, weak, wide-blocksize block cipher.

17. A cipher as recited in claim 16, wherein the weak, wide-blocksize block cipher is a mode of operation of a conventional block cipher.

18. A cipher as recited in claim 16, wherein at least one of said steps depends on a tweak.

19. A cipher as recited in claim 16, wherein said masking step uses multiplication in a finite field.

20. A cipher as recited in claim 16, wherein said masking step uses a mask obtained by XORing together portions of the intermediate value.

21. A method of enciphering by a wide-blocksize block cipher having a blocksize of mn bits, wherein the wide-blocksize block cipher is constructed using a conventional block having a blocksize of n bits, comprising:

using the conventional block cipher in a mode of operation to compute an intermediate value;

masking the intermediate value; and

using the conventional block cipher in a mode of operation to compute the final ciphertext.

22. A method as recited in claim 21, wherein at least one of said steps depends on a tweak.

23. A method as recited in claim 21, wherein said masking step uses multiplication in a finite field.

24. A method as recited in claim 21, wherein said masking step uses a mask obtained by XORing together portions of the intermediate value.

25. A method of producing a wide-blocksize block cipher from a conventional block cipher, comprising:

converting the conventional block cipher into a first, weak, wide-blocksize block cipher using a first mode of operation of said conventional block cipher;

converting the conventional block cipher into a second, weak, wide-blocksize block cipher using a second mode of operation of said conventional block cipher; and

transforming the output of the first mode of operation into the input of the second mode of operation by a mixing operation.

26. A method as recited in claim 25, wherein at least one of said steps depends on a tweak.

27. A method to protect the privacy of data stored on a mass-storage device that is organized into a sequence of sectors, each sector having a unique sector index, some or all of the sectors being ciphertexts, each ciphertext being the encryption of a plaintext under a given key and depending on the sector index, comprising:

forming each said ciphertext by

using a block-cipher mode of operation to transform the plaintext into an intermediate value;

mixing the bits of the intermediate value using a mixing transformation; and

using a block-cipher mode of operation to transform the mixed intermediate value into the ciphertext.

28. A method as recited in claim 27, wherein at least one of said steps depends on a tweak.

29. A computer-readable storage medium, said storage medium storing instructions that when executed by a computer cause the computer to encipher a plaintext according to the operations comprising:

enciphering the plaintext with a weak, wide-blocksize block cipher to produce an intermediate value;

masking the intermediate value to produce a masked intermediate value; and

deciphering the masked intermediate value using a weak, wide-blocksize, block cipher.

30. A storage medium as recited in claim 29, wherein the weak, wide-blocksize block cipher is a mode of operation of a conventional block cipher.

31. A storage medium as recited in claim 29, wherein at least one of said operations depends on a tweak.

32. A storage medium as recited in claim 29, wherein said masking operation uses multiplication in a finite field.

33. A storage medium as recited in claim 29, wherein said masking operation uses a mask obtained by XORing together portions of the intermediate value.

34. A wide-blocksize block-cipher enciphering apparatus that is configured to use a conventional block cipher and a key to encipher a plaintext into a ciphertext, comprising:

a programmable computer; and

programming executable on said computer for carrying out the operations of

enciphering the plaintext with a weak, wide-blocksize block cipher to produce an intermediate value;

masking the intermediate value to produce a masked intermediate value; and

deciphering the masked intermediate value using a weak, wide-

blocksize, block cipher.

35. An apparatus as recited in claim 34, wherein the weak, wide-blocksize block cipher is a mode of operation of a conventional block cipher.

36. An apparatus as recited in claim 34, wherein at least one of said operations depends on a tweak.

37. A method as recited in claim 34, wherein said masking operation uses multiplication in a finite field.

38. A method as recited in claim 34, wherein said masking operation uses a mask obtained by XORing together portions of the intermediate value.

40. A secure disk drive, the disk drive organized into a sequence of sectors, the contents of some or all of the sectors being encrypted depending on a key, a plaintext value, and the index of the sector within the sequence of sectors, at least one said sectors being encrypted by a process comprising:

enciphering plaintext using a first enciphering scheme which forms an intermediate value;

masking the bits of the intermediate value and forming a masked intermediate value;

deciphering the masked intermediate value using a second enciphering scheme which thereby forms the encrypted sector.

41. A secure disk drive as recited in claim 40, wherein at least one of said steps depends on a tweak.

42. A secure disk drive as recited in claim 40, wherein said masking step uses multiplication in a finite field.

43. A secure disk drive as recited in claim 40, wherein said masking step

uses a mask obtained by XORing together portions of the intermediate value.

44. An enciphering method, comprising:

computing a first intermediate value from a plaintext;

computing a mask from the first intermediate value;

computing a second intermediate value from the first intermediate value and the mask; and

computing a ciphertext from the second intermediate value.

45. A method as recited in claim 44, further comprising:

computing said second intermediate value from said ciphertext;

computing said mask from said second intermediate value;

computing said first intermediate value from said second intermediate value and said mask; and

computing said plaintext from said first intermediate value.

46. An enciphering method, comprising:

computing a first intermediate value from a ciphertext;

computing a mask from the first intermediate value;

computing a second intermediate value from the first intermediate value and the mask; and

computing a plaintext from the second intermediate value.

47. A method as recited in claim 46, further comprising:

computing said second intermediate value from said plaintext;

computing said mask from said second intermediate value;

computing said first intermediate value from said second intermediate value and said mask; and

computing said ciphertext from said first intermediate value